Secure Smart Homes: Opportunities and Challenges

JORDI MONGAY BATALLA, National Institute of Telecommunications,
Warsaw University of Technology, Poland
ATHANASIOS VASILAKOS, Lulea University of Technology, Sweden
MARIUSZ GAJEWSKI, National Institute of Telecommunications, Poland

The Smart Home concept integrates smart applications in the daily human life. In recent years, Smart Homes have increased security and management challenges due to the low capacity of small sensors, multiple connectivity to the Internet for efficient applications (use of big data and cloud computing), and heterogeneity of home systems, which require inexpert users to configure devices and micro-systems. This article presents current security and management approaches in Smart Homes and shows the good practices imposed on the market for developing secure systems in houses. At last, we propose future solutions for efficiently and securely managing the Smart Homes.

CCS Concepts: • **Security and privacy** → **Security services**;

Additional Key Words and Phrases: Smart Home, constrained devices, security, wireless sensor networks

ACM Reference format:
Jordi Mongay Batalla, Athanasios Vasilakos, and Mariusz Gajewski. 2017. Secure Smart Homes: Opportunities and Challenges. *ACM Comput. Surv.* 50, 5, Article 75 (September 2017), 32 pages.
https://doi.org/10.1145/3122816

1 INTRODUCTION

1.1 Motivation

The Smart Home concept is the answer to the demand of integration of smart appliances and systems in the human environment. It encompasses a rising number of devices, services, and applications that make people's life and everyday duties easier. Based on a dozen technologies and standards, hundreds of device suppliers offer an extensive range of solutions (meters, actuators, sensors, micro-systems, etc.) that are integrated in the Home environment. This heterogeneity directly affects the increase of security problems in the Smart Homes.

Even if vendors try to agree on good practices in security implementation, the reality is that the interconnection of devices provided by different vendor already presents a number of issues

This work was undertaken under the PolLux IDSECOM project and the PolTur FUSE project supported by the National Centre for Research and Development (NCBiR) in Poland.

Authors' addresses: J. M. Batalla, National Institute of Telecommunications, Szachowa 1, 04-894 Warsaw, Poland; Warsaw University of Technology, Nowowiejska 15/19, 00-665 Warsaw, Poland; email: jordim@interfree.it; A. Vasilakos, Lulea University of Technology, SE-971 87 Luleå, Sweden; email: athanasios.vasilakos@ltu.se; M. Gajewski, National Institute of Telecommunications, Szachowa 1, 04-894, Warsaw, Poland; email: M.Gajewski@itl.waw.pl.

https://doi.org/10.1145/3122816

in regard to security and privacy. Moreover, many of the devices classified into the Internet of Things (IoT) have limited resources (from the point of view of processing capacity and storage), which makes the execution of complex security mechanisms difficult.

In the last years, two more worrisome (from the point of view of security achievement) tendencies have appeared while building Smart Homes. The first one is the multiple connectivity to the Internet. This is caused by the cloud-based management of IoT systems as well as by the use of the cloud systems as collaborators of IoT, i.e., many IoT systems make use of the cloud for data analysis and storage.

The second tendency is the behavior of end users, who are becoming responsible for configuration of Smart Home functions including setting access passwords, granting access to devices or services (i.e., electronic door locks). This may cause security holes and instability in the Smart Home environment.

1.2 Main Contributions

The current situation of Smart Home environments requires new solutions for providing security and data privacy. Data privacy is another hot topic in Smart Homes since a number of critical applications have been brought to the houses, e.g., a smart health.

In this article, we present the current approaches to security in Smart Homes, including standards and outstanding mechanisms. We describe security issues, grouping them in different objectives (integrity, privacy, availability, etc.), which are closely related to Smart Home environment. We present threats and countermeasures used in current systems. Moreover, we look at the security from a practical point of view and describe the current practices (called *good practices*) for ensuring security goals within heterogeneous Smart Home systems.

Finally, we compile the open research issues and expound how Smart Homes will develop in the future.

2 THE SMART HOME CONCEPT

Recently, an increasing number of homes have been equipped with smart devices that interact with the inhabitants, observing and learning their behavior and providing proactive services on that basis. They are designed to provide more comfort, strengthen the feeling of safety, help to manage energy, etc. Until quite recently, all these applications were an isolated island (from the point of view of technology), each one operating with several devices generally communicating in the same radio space. Nowadays, each household constitutes an ecosystem where all the devices cooperate, offering different services and sharing the radio space.

In principle, this approach can be modeled by two layers within the Home Area Network (see Figure 1 for details), the lowest one containing communication with and between the devices and the highest one containing composed services exposition. By the term *Home Area Network (HAN)*, we understand all the devices and communication rules operating jointly in the house scope for creating the Smart Home reality. HAN assumes connectivity with external systems (*Wide Area Network*). The HAN comprises the following components:

- The set of Internet of Things (IoT) devices, which control various aspects of human existence (in-home and in the nearest surrounding) by using different devices. Some studies also distinguish constrained devices and powerful equipment (e.g., [1, 2]), where:
  - constrained devices are devices with limited power, memory, and processing resources strictly tailored to concrete tasks (i.e., smart bulbs, smart meters, sensors, etc.). For this reason, the implementation of additional processes (including security) is considerably difficult or impossible. According to report by Lévy-Bencheton et al. [1], constrained

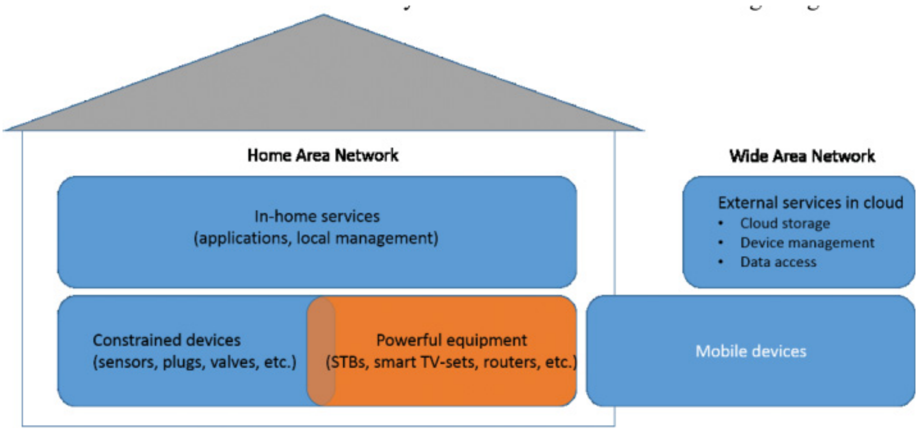

Fig. 1. Smart Home environment and its relationships.

devices might be divided into several categories depending on their RAM capacity, memory storage capacity, and CPU power. Indeed, the class of a constrained device has an impact on its security capabilities, and thus it introduces limits to the application of security mechanisms.

  - powerful equipment are devices typically powered by the main supply which may offer enough computational power, memory, and communication interfaces to perform additional tasks including security. Examples of powerful equipment are Home Gateway (HG), TV sets, and the like.
- In-home services which allow HAN to control the IoT devices and present gathered data. These services usually expose interfaces to manipulate device settings and present the measured parameters or status of constrained devices. The services might be accessed by external applications through a local web server.
- Remote services including remote (multimedia) content storage, device administration, and analytics. They ensure the access to all or selected management functions. Moreover, these services often provide storage for backup and user data (e.g., shared multimedia files).
- At last, mobile devices are often used to control remotely the Smart Home, including remote activation of services. They make use of remote services for getting access to in-home services.

IoT devices can form a network, becoming “constrained nodes” in that network [2]. Such a network may suffer from several important constraints such as unreliable channels, limited and variable bandwidth, and a highly dynamic topology. The communication between constrained network and other networks is usually maintained by way of gateways (often called *hubs* or *smart hubs*), which ensure conversion of transmission medium and communication protocols, and often play the role of storage unit for exchanging data. In small deployments, conversion processes may be performed by one device – Home Gateway, which usually serves as a router, firewall, WiFi access point, and command center for controlling all devices constituting the Smart Home ecosystem. In more complex solutions, the devices are usually grouped by technologies (e.g., ZigBee, Z-Wave, etc.), functionalities (e.g., heating, lightening, sensing, etc.) or location (e.g., floor inside of a building). Constrained devices are connected to HAN through controllers, signal repeaters and other transmission devices which support communication.

2.1 Application Areas of Smart Home

Smart Home concept enables the management and control of different functional areas related with the comfort of the inhabitants. The functional areas may be divided into (but are not limited to) five groups: energy efficiency, renewable energy, e-health, multimedia, and surveillance & security [3–6].

2.1.1 Energy Efficiency and Management. One of the aims of introducing Smart Homes was the need for reducing energy consumption by households. At the basic level, this involves gathering energy consumption data coming from various home appliances (called *smart metering*) and introducing event-based energy saving procedures (e.g., energy saving when inhabitants are not at their home). The further development of home automation tools gave the ability to better match the energy consumption with the lifestyle and habits of the household. They apply logic in controlling home appliances as well as advanced dashboards to provide feedback about energy usage. In this context, smart energy control systems can monitor the home energy consumption and find intelligent solutions for energy saving within the house.

2.1.2 Renewable Energy Management. Energy management in broader sense includes also the use of renewable energy sources. Therefore, the Smart Home concept might include the use of solar, wind, and other renewable energy sources. In this case, the alternative energy sources must be integrated within a power consumption management mechanism. This is particularly important if the energy suppliers plan to distribute electricity obtained from renewable sources within Smart Grids [7]. In the market, there are several commercial solutions for home energy management services which include differentiated energy sources (e.g., Honda Smart Home[1] and Bosch Smart Home[2]).

This set of Smart Home functionalities combined has a great impact on the Smart Grid deployment which encompasses all actors on the energy market.

2.1.3 Health Care Systems. Smart Home environment is also open for personal constrained devices used as clothing or accessories – wearables. Their rising popularity also impacts the Home Area Network concept. The possibility of monitoring physical health is one of the key features attracting users. Health monitoring is necessary in an aging society. In this context, Smart Home systems supporting healthcare can complement or even replace selected current high-cost hospital healthcare practices. Moreover, wearables and other healthcare technologies help older people to live independently in their own houses [8], reducing the expenses of clinic-based assessments and labor-intensive procedures [9].

2.1.4 Advanced Multimedia Services. Recently, the number and variety of multimedia applications used by inhabitants within the Smart Home has grown significantly. It has resulted from the increasing popularity of mobile devices, entertainment platforms (e.g., Game consoles, Media centers, etc.). On the other hand, all of these devices need to be attached to the home network to share multimedia or support control over the media environment. As a result, recent years have seen big changes in the approach to home entertainment. Mendes et al. [10] argued that the evolution of future Home Area Media Networks (HAMNs) is constantly driven by an expectation that the future media parameters will go beyond the current high-definition formats. On the other hand, the media has become more interactive than it was earlier, which results in the introduction of smart TV sets, smart set top boxes, and other similar devices. The HAMN trend aims at connecting various families of smart devices (TV sets, set top boxes, media centers, network hard drives,

[1] http://www.hondasmarthome.com/.
[2] https://www.bosch-smarthome.com/.

game consoles, etc.) in one ecosystem, providing entertainment for all household members. However, generational differences create also a barrier for the use of multimedia devices in the house, so not all the household members profit from the HAMN, as explained in [11] and [12].

2.1.5 Surveillance and Security. Surveillance and security systems are intended to gather accurate data for further processing (e.g., face and object recognition, human activities recognition). Therefore, these services often require QoS support adequate for carrying out the computations related to image analysis [13]. Not all the surveillance methods are applicable to Smart Home environments because of computational complexity and required short delay for intrusion event detection. Moreover, Smart Home network infrastructure usually does not support transmission from multiple high-definition cameras. Instead of this, home surveillance cameras served by constrained nodes share the limited network resources and transmit the video signal to the storage for further processing. Solutions for such systems have been presented in [14] and [15] as well as similar systems addressed to face recognition and sound localization that have been presented in [16].

2.2 Home Area Network (HAN)

The Smart Home concept assumes that the devices constituting the ecosystem are connected in one or more Home Area Networks (HAN), which include:

- One or several High-Speed Networks, usually Wi-Fi Networks that may be provided by a set top box, mobile devices, gateways, access points, and the like.
- Personal Area Networks or ad-hoc networks created between several constrained devices, for instance, using low-speed connections (Bluetooth, ZigBee, Z-Wave, etc.). This concept comprises also the Wireless Sensor Networks (WSNs).

The use of High-Speed Networks in context of smart devices relates mainly to the user access. The most common method of smart device manipulating is through a web browser or a dedicated smartphone application (via dedicated vendor's server or cloud service). More powerful devices offer access through their own built-in web server, which allows the user to use a web-based GUI to manipulate the appliance. Other groups of devices expose their own API that the user can interact with. In this case, smart device exposes an API directly or using other resources.

Servers exposing APIs may reside on the HG or may be run in the cloud. The advantages of the clouds are that they provide whole solutions (to Smart Home software providers) without the necessity of building and, in addition, the clouds support unifying security tools (e.g., patches and firmware updates) as well as analytic tools. In turn, exposing API service within HAN requires also running a listener service on a specified port. Although launching this service from HAN is usually not a problem, for the remote access (over the Internet) port forwarding on HG and the appropriate security policies must be applied.

Besides HAN, the Smart Home ecosystem ensures connections to Wide Area Networks (WAN), including (1) High-Speed Networks, typically providing access to the Internet, for instance through the Internet Service Provider (ISP) network or the Mobile Network Operator (MNO) network, and (2) Low-Power Wide Area Networks (LPWAN), which are also able to provide WAN connectivity while requiring low power from the end nodes (e.g., LoRaWAN,[3] Sigfox,[4] etc.).

[3] https://www.lora-alliance.org.
[4] http://www.sigfox.com/.

Essentially, communication with WAN aims at exposing managing interfaces. For this reason, specialized software companies such as Belkin's WeMO, iControl networks,[5] and Zonoff[6] focus on development of IoT-related software platforms responsible for managing different wireless communication protocols and standards, cloud computing, and data storage. These platforms expose APIs addressed to control the Smart Home components.

2.3 Communication Standards for HAN

Popular HAN solutions are based on radio and cable (mostly Power Line Communication – PLC) standards. The radio communication within HAN is mainly based on standards presented in Table 1.

Cable-based communication systems for HAN include standards based mainly on X10, which describes the powerline signaling technology.

Home Automation Networks make also use of communication suites, which encompass standards for multiple types of physical layer (both power line and radio communication). The most popular solutions come from home automation industry and include both open and proprietary solutions. Some popular examples are:

- Insteon, which is the patent-protected technology, wherein the radio communication uses similar band as Z-Wave but at different frequencies across different countries (Z-Wave: 868.42MHz – 921.42MHz, Insteon: 869.85MHz – 921MHz). The powerline version operates at 131.65kHz. It's also compatible with X10 solutions.
- LonWorks, which is the communication standard created by the Echelon Corporation. It uses different media types such as twisted pair, coaxial cables, power lines, fiber optics, infrared, and radio. The standard defines the communication rules at the seven layers of the OSI (Open Systems Interconnection) model.
- The KNX standard, which unifies the three existing standards: the European Installation Bus (EIB), European Home Systems Protocol (EHS), and BatiBUS. It describes communication rules using several physical media types, including: twisted pair, powerline (inherited from EIB and EHS), radio (KNX-RF, which operates at the 868MHz), infrared and Ethernet.

The aforementioned standards cover most popular communication platforms used in HAN. However, it should be noted that their use extends far beyond the home automation.

3 SECURITY APPROACHES IN SMART HOME

General security requirements for Smart Home infrastructure cover six well-known goals: confidentiality/privacy, integrity, authenticity, non-repudiation, availability, and authorization. However, unlike Internet-connected terminals, most Smart Home equipment neither have a uniform execution environment nor enough computational power. Therefore, it is difficult to implement a complex security strategy. Since the Smart Home environment partially inherits its components from IoT systems, some security-related categories describing IoT platforms may also be applied to Smart Homes, specifically as regards the WSNs. WSN architecture has been developed with particular emphasis on security issues [17, 18] and includes the:

- Perceptual layer consisting of all devices gathering information about physical world as well as impacting on the environment;

[5] https://www.icontrol.com/.
[6] https://zonoff.com/.

Table 1. Popular Radio Communication Standards for HAN

Standard/reference	Subject
IEEE 802.15.4	Standard for Low-Rate Wireless Personal Area Networks (WPANs), which defines both the physical (PHY) and the Media Access Control (MAC) layers. The first version (issued in 2003) made use of the Direct Sequence Spread Spectrum (DSSS) technique, but the successive releases extended the scope of application for other spread spectrum methods and different modulations. This standard is used by several higher layer protocols such as ZigBee,[7] 6LoWPAN.
Z-Wave	Standard for wireless communication protocol, which operates in the Part 15 unlicensed industrial, scientific and medical band (at 868.42MHz in Europe). This standard is supported by the Z-Wave Alliance as competitor/replacement for ZigBee
Bluetooth Low Energy (BLE)	Standard for wireless communication over short distances, defined by the Bluetooth SIG (Special Interest Group[8]). It operates in the unlicensed ISM 2.4-GHz band and is used as ad-hoc point-to-point PAN technology. The radio communication is based on Frequency Hopping Spread Spectrum (FHSS) for avoiding occupied frequencies. It offers up to 1Mb/s over 1MHz channels using this technique.
EnOcean	The wireless communication suite standardized by the International Electrotechnical Commission (IEC) and supported by the EnOcean Alliance.[9] It defines transmission in four bands: 902MHz, 928.35MHz, 868.3MHz, and 315MHz.
WiFi, (IEEE 802.11 standards group)	IEEE 802.11 uses the following PHY radio techniques: DSSS, FHSS, OFDM (Orthogonal Frequency Division Modulation). Currently, the most widely used versions are 802.11a and 802.11g. Both of them provide theoretical 54Mb/s using CSMA/CA, wherein the "a" version is based on transmission in the 5GHz band. The latest versions (802.11n and 802.11ac) increase the maximum data rates to 150Mb/s and 866.7Mb/s, respectively. WiFi standards are used as a basic communication method used by many Smart Home devices manufacturers, i.e., Belkin's WeMo,[10] Apple's HomeKit.[11]

- Network layer ensuring the reliable transport of data from perceptual layer, its initial processing in constrained devices or gateways, proper classification, and conversion of the data form. It encompasses data exchange across various networks, i.e., local, access (wired, wireless – mobile network) and core network;
- Application layer providing customized services according to the user needs. Some authors distinguish an additional layer called support layer, which is aimed at setting up the support platform for the application layer, in terms of preparation and organization of IoT data. In this context, the support layer would be responsible for data computation, aggregation and access for the application layer;

[7] http://www.zigbee.org/.

[8] http://www.bluetooth.org.

[9] https://www.enocean-alliance.org/.

[10] http://www.belkin.com/us/Products/home-automation/c/wemo-home-automation/.

[11] http://www.apple.com/ios/homekit/.

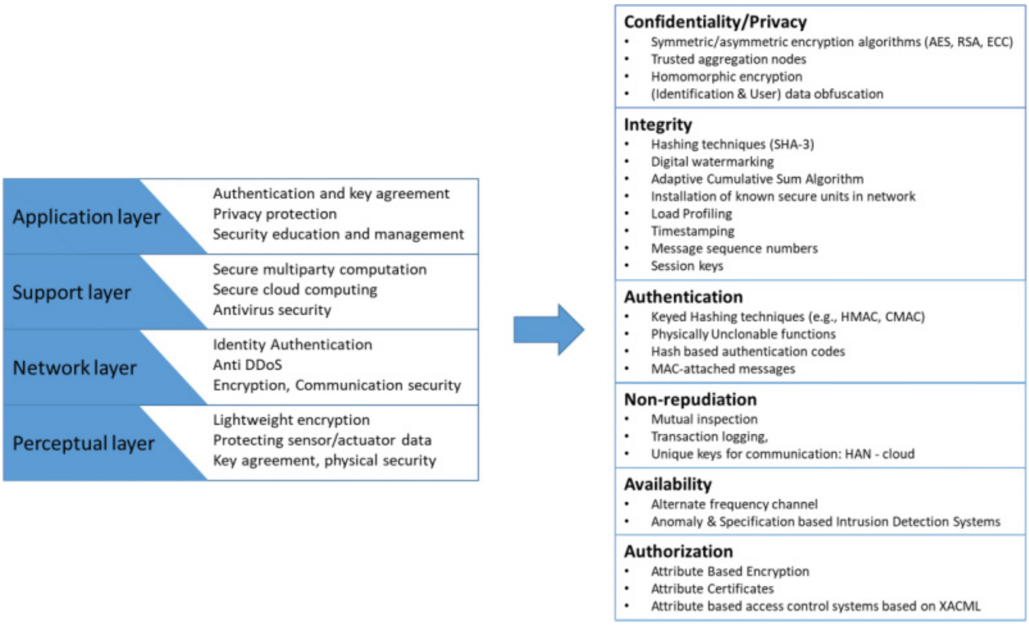
Application layer
Authentication and key agreement
Privacy protection
Security education and management
Support layer
Secure multiparty computation
Secure cloud computing
Antivirus security
Network layer
Identity Authentication
Anti DDoS
Encryption, Communication security
Perceptual layer
Lightweight encryption
Protecting sensor/actuator data
Key agreement, physical security
Confidentiality/Privacy
Symmetric/asymmetric encryption algorithms (AES, RSA, ECC)
Trusted aggregation nodes
Homomorphic encryption
(Identification & User) data obfuscation
Integrity
Hashing techniques (SHA-3)
Digital watermarking
Adaptive Cumulative Sum Algorithm
Installation of known secure units in network
Load Profiling
Timestamping
Message sequence numbers
Session keys
Authentication
Keyed Hashing techniques (e.g., HMAC, CMAC)
Physically Unclonable functions
Hash based authentication codes
MAC-attached messages
Non-repudiation
Mutual inspection
Transaction logging,
Unique keys for communication: HAN - cloud
Availability
Alternate frequency channel
Anomaly & Specification based Intrusion Detection Systems
Authorization
Attribute Based Encryption
Attribute Certificates
Attribute based access control systems based on XACML

Fig. 2. Security requirements vs countermeasures in general IoT architecture.

This architecture is also directed to solve the security problems existing from the bottom (individual devices) to the top (IoT services), such as physical security of devices and communication between them, data acquisition security, and information processing security. The measures adopted for achieving the security goals and their division into the architecture stack are presented in Figure 2.

The security requirements assigned to a given layer of the architecture are closely related to the features offered by the layer. At the *perceptual layer,* lightweight encryption technology becomes important for protecting the devices. This encryption should include lightweight cryptographic algorithms and lightweight cryptographic protocols for symmetric (or asymmetric, if possible) cryptography. Moreover, applied cryptography mechanisms should also include tools for ensuring the integrity and authenticity of exchanged sensor/actuator data.

At the *network layer* (called also the *transportation layer*), ambiguous security mechanisms on the end-to-end path are inapplicable because of constraints of HAN network nodes. HAN nodes require an authentication process to prevent information from being exchanged with illegal nodes. Therefore, the network layer also needs to provide mechanisms for confidentiality and integrity of exchanged data. It should convince suppliers to prevent the constrained network from the possibility of attaching a node for introducing a distributed denial of service attack (DDoS). Some researchers point out that this threat is common in the network layer and may have serious implications particularly in the IoT [18]. Thus, prevention methods from the DDOS attacks should also be provided at this layer.

Security requirements for the *support layer* result from the needs generated by applications used in communication within the HAN such as cloud computing and various secure distributed computation models. In this regard, the requirements of the strong encryption algorithms and protocols derived from those models (cloud and distributed computation) should be applied to HAN devices and data (including application security technologies and anti-virus).

At the *application layer*, security requirements are focused on two aspects: the first one concerns the applied authentication procedures and the use of key agreement mechanism across the heterogeneous network and the second one deals with ensuring the privacy of end-users. In this context, Suo et al. [18] also draw attention to the end-user education related to the security aspects.

The three-layer security model presented above is aligned with the general reference architecture proposed by the EU FP7 IoT-A project. Particularly, the IoT-A structure known as Architectural Reference Model for the IoT – ARM [19] defines all the essential building blocks and design options in areas such as system functionality, performance, deployment rules, and security. One of the sub-models of the ARM is a Security Model which is related to the functionalities and interactions needed. The IoT-A Security Model is built on three pillars: Trust, Security, and Privacy, where Security distinguishes among service security, communication security, and application security. This model should be treated as a set of security features because target architectures can exhibit different approaches, depending on the actual needs [19].

In Smart Home environments, the security mechanisms are difficult to implement because: (1) HAN is a heterogeneous ecosystem that integrates several types of devices, services, and technologies; (2) most of the devices are designed to perform strictly assumed functionality and therefore usually have limited security support because of their weak capacities (CPU, battery, etc.); and (3) many devices (or systems comprised of these devices) are interfaced with remote infrastructures (cloud storage, analytics, or remote access to the devices) to offer their services. Many organizations have tried to standardize selected aspects of device cooperation within the Smart Home (i.e., oneM2M,[12] LightweightM2M[13]). When it comes to security, the most comprehensive model (taking into account several options) has been developed within the IoT-A EU project. In addition, the security mechanisms used in popular IoT cloud platforms like Xively and HomeKit align some entities that were defined within the ARM model introduced by the IoT-A project. The integration and implementation of a subset of functional blocks has been realized under the FP7 SMARTIE EU project, which performs in comprehensive manner the adaptation of the model to the smart city concept.

In SMARTIE, several software components have been developed for helping the users to better protect IoT systems at various levels, especially taking into account constrained nodes. Specifically, lightweight encryption, node credentials, and lightweight generation of pseudo-randomness have been proposed to offer better protection to constrained nodes. Moreover, the SMARTIE system offers encryption functionality linked with access control mechanism. This is especially beneficial when multiple receivers are involved. The information is encrypted once according to the access policy, ensuring that all authorized recipients can decrypt the messages. The system offers enablers for authentication and authorization targeted at several use cases from constrained to powerful devices. The novelty is that the enablers may execute certain processing functionalities directly on the encrypted data.

Similarly, the goal of FP7 RERUM project was to enhance the trustworthiness of IoT technologies by adopting the concept of "security, privacy, and reliability by design". The project developed architectural and communication frameworks for the interconnectivity of a large number of heterogeneous smart objects within the city. The proposed frameworks extend security functionalities defined by the ARM Model, thanks to the definition of security primitives that may be developed in restricted devices within a controlled environment.

[12] ETSI SmartM2M provides specifications for M2M services and applications, focusing on aspects of the IoT aspects and Smart Cities (http://www.etsi.org/technologies-clusters/technologies/internet-of-things).

[13] LWM2M (OMA LightweightM2M) is an industry standard for device management. It relies on CoAP protocol and therefore is optimized for communications over sensor or cellular networks.

With regard to security issues, the ARM Model was created for IoT as a generalized set of security functional blocks and not as a detailed model. In this context, the ENISA report [1] proposes a comprehensive categorization of Smart Home threats as a starting point for discussion.

4 THREATS

Based on the presented 3-layer software stack and following, in part, the ENISA taxonomy published in [1] and [2], we may classify the security threats to the HAN devices as threats against privacy, services availability, proper operation, authorization data leakage/misuse, altering of stored data, interception of information, and repudiation of actions. According to both reports [1, 2], the Smart Home environments may suffer from threats (limited to hardware/software/communication) categorized as follows:

- Privacy/security threats including both nefarious activity (abuse) and Eavesdropping/Interception/Hijacking, where leveraging design or implementation flaws. The attacker is able to compromise one or several assets, provoking loss of confidentiality of private data or loss of control over a device;
- Physical attacks on smart devices related to manipulation of devices. These attacks are typical in IT and may consist of uploading new firmware, adding hardware components, changing device settings, extracting encryption keys, and so on;
- Disasters and outages, which cover cases including denial of service for the user;
- Damage/loss (IT assets), which cover risks related to the removal of vulnerable data from unused devices.

The following sections discuss main threats categories in the context of the individual layers of the described model.

4.1 Perceptual Layer

This group introduces threats in the smart device's surrounding that are technology dependent (see Table 2).

Although communication standards provide necessary security mechanisms, suppliers do not always implement them for fear of losing stability/performance in difficult propagation conditions. In this context, test results presented in reports prepared by Cognosec [20] outline that some ZigBee devices practically do not offer secure communication. Also selected implementations of the Z-Wave standard suffer from lack of security, as shown by the group black hat hackers in the U.S. They intercepted, impersonated, and finally disabled devices communicating with Z-Wave[14] within the Smart Home. Similarly, the UK researchers found exploited security loopholes in the implementation of cryptographic libraries. It turned out that the set of functions used for authentication of HAN devices was vulnerable to attacks. Zillner [20] have compromised home automation controllers. Moreover, they were able to take control over the remotely accessible devices including such safety-critical appliances as door locks and alarm systems. As it turned out further, the transmission between Z-Wave nodes was secured using an encryption algorithm that was hidden in the source code running the communication protocol. The researchers were able to extract the secret key from the Z-Wave packet exchange by the protocol reverse engineering.[15]

[14] http://www.securityelectronicsandnetworks.com/articles/2015/11/19/considerations-z-wave-intrusion-detection-systems.

[15] https://sensepost.com/cms/resources/conferences/2013/bh_zwave/Security%20Evaluation%20of%20Z-Wave_WP.pdf Security Evaluation of the Z-Wave.

Table 2. Threats at the Perceptual Layer

Threats category	Threats	Characteristics/ attack examples
Nefarious Activity/ Abuse	Identity theft of the device	At the perceptual level, this threat consists in taking control of the smart device. One of the possible attacks might make use of the device-dependency of the pre-loaded encryption keys and might be performed on the ZigBee devices paired with the smart hub [20]. A similar vulnerability for attacks demonstrate devices that use Z-Wave radios. A new device joining a network uses a hardware-based pseudo-random generator and a temporal hard-coded default-bit pattern for generating a symmetric key. A potential attacker is able to sniff the initial device pairing exchange and steal the generated encrypted key [21].
	Malicious code/software activity	This group of threats encompasses attacks based on applying the malicious code on smart devices software. The possibility of using these methods is strongly determined by smart device hardware and software construction.
	Abuse of information leakage	This group of threads is mainly related to privacy leakages through smart device traffic analysis. Most attacks are carried out against radio devices since wireless communication technologies are prone to such threats. As a result, they might lead to obtaining confidential information which combined with social media information reveal sensitive data describing residents of the house. Attacks are usually analyzed by vendors and used for software updates. An example is the susceptibility to hacks of the BLE-powered smart locks which send a user's password in plain text to a smartphone.[16]
	Manipulation of hardware & software	According to [1], this threat group relates to unauthorized physical manipulation during the whole life cycle of the smart device, including the production process. Exemplary threat, researched and described by [22], refers to malicious hardware modification during fabrication process. It also includes manipulations caused by poor physical security at the exploitation phase, which makes it feasible that a potential attacker accesses, e.g., USB ports or SD cards readers, to access the operating system and potentially any data stored on the devices (one of the major HAN threats outlined by the Open Web Application Security Project[17]). Manipulation may also be performed by using a configuration client installed by an impersonating attacker.
	Manipulation of information	Following the taxonomy presented in [1], this group of threats encompasses attacks against non-repudiation of information processed by HAN-connected devices. In consequence, it may lead to the repudiation of performed actions, logs modifications, etc.
	Misuse of audit tools. Falsification of records	Audit tools are common for the system development process, however they may be used also by attackers. This group of threats includes also misuse of the information obtained by physical protocol sniffers.

(Continued)

[16] http://www.digitaltrends.com/home/bluetooth-smart-locks-easily-hackable/.
[17] https://www.owasp.org.

Table 2. Continued

Threats category	Threats	Characteristics/ attack examples
	Unauthorized installation of Software. Badware	The exemplary attacks encompass writing the modified firmware to the victim,s device. Examples of attacks that use infected firmware updates through the USB port are presented in [23]. Arias et al. point out that tested devices did not use encrypted nor digitally signed firmware for updates, making them susceptible to change for an potential attacker.
Eavesdropping / Interception / Hijacking	Interfering radiations	This threat category refers to wireless networks and encompasses attacks launched at physical layer. The most common example of the attack that might lead to the radio channel disruption is jamming [24]. It is based on interference of the attacker's station with the radio frequencies of the nodes.
	Interception of information. Network reconnaissance and information gathering, Replay of messages, Man in the middle/ session hijacking	The interception of transmitted information is relatively easy in the case of radio communication. The various radio standards support payload encryption at the link, or at the upper protocol layers (i.e., WiFi, IEEE-802.15.4-based technologies, Z-Wave, BLE). On that basis the potential attacker may perform time analysis and traffic burst correlation as well as traffic shape analysis, which may help in device identification (e.g., smart TV, NAS repository, etc.). Next, combined with observed user behavior, this information may be used to profile the house occupants' habits. On the other hand, sniffed packets might be used for replay traffic attacks aimed at destabilizing the system. Into this category falls also a broad range of relay attacks. Particularly, various radio controlled smart locks are vulnerable to those attacks. Example of the Bluetooth relay attacks launched on smart locks may be seen in [25].
	Repudiation of actions	This threat category refers to the intentional data manipulation to repudiate action taken by the smart device. In literature, the common example is based on attacks against non-repudiation of smart grids metering data [26].
Physical attacks		This threat category encompasses a wide spectrum of physical attacks on smart devices. The most representative example is tampering, which refers to the physical attacks on the sensor nodes [27]. Physical attacks may cause damage to the sensors or may make them completely unserviceable. Many examples in literature show that the threat may turn out to be more feasible with an increasing number of sensors in our environment. [28]. Moreover, physical attacks on the sensors could also threaten to bring down the entire sensor network by destroying, disabling, or stealing the sensors.
Dependability and reliability	Outages/Disasters	This threat category encompasses events directly causing smart device to lose service. In [1], Lévy-Bencheton et al. point out exemplary situations such as lack of electricity. An intentional action taken by an attacker may make selected/all smart home devices unavailable.
	Failures/ Malfunctions	This category encompasses threats arising from failures and malfunctions mainly caused by: • hardware and software bugs, • failures of communication links (e.g., between devices and the smart hub), • failures or disruptions of power supply, • configuration errors, etc.

4.2 Network Layer

Generally, this category encompasses threats related to the end-to-end communication including also communication over the Internet (see Table 3).

The range of the constrained devices' end-to-end communication is often limited by the technology that is used. Particularly, radio technologies require data passing through gateways with connectivity to IP-based world. It reduces susceptibility to various security risks that might compromise transmitted data, because end-to-end data exchange (on behalf of the constrained device) is performed by powerful (home) gateway, which is able to secure the transmission over the IP network.

4.3 Application Layer

At the application layer threats encompass security violations related to application logic, data processing, and reasoning. Table 4 gives information about main categories of threats and provides examples of security vulnerabilities.

The above threats classification concentrates on various aspects of Smart Home data accessing and processing. It covers actions taken both by smart device and cloud infrastructure.

Threats concerning the data manipulation through web interface (based on local resources or vendor's cloud) were characterized by OWASP (see Table 4) but may be extended also on smart-device APIs.

On the other hand, cloud environment performing smart device data processing is exposed to typical threats for those solutions. It ranges from physical outages, account/service traffic hijacking (leading to data loss), insecure APIs (including bugs), DoS attacks, malicious insider attacks, and the like.

5 COUNTERMEASURES

Current HAN deployments are based mostly on wireless communication. Because of its broadcast nature, the wireless communication is susceptible to eavesdropping and various active attacks. Also Internet connectivity may make that Smart Home infrastructure vulnerable to attacks. Wireless connections and Internet access together with the constrained condition of the devices are the weakest security points in Home Smart environment and, because of them, all the contexts of security are at risk, i.e., confidentiality/privacy, integrity, authenticity, non-repudiation, availability, and authorization. Therefore, the countermeasures that need to be taken are related to all the security contexts.

5.1 Confidentiality/Privacy

In the context of the communication within the HAN infrastructure, confidentiality assumes that exchanged user data are properly protected on the link between the constrained devices and the sink node. The use of encryption keys in HAN deployments raises significant problems related to both enormous resource consumption and efficient distribution of encryption keys. A common approach assumes that the cryptographic keys are distributed across the constrained devices before the network is deployed (Static Key management). Another solution is known as Dynamic Key management and assumes that encryption keys are distributed to the constrained nodes on demand and this process is triggered by the so-called keying events.

Table 3. Threats at the Network Layer

Threats category	Threats	Characteristcs/ attack examples
Nefarious Activity/ Abuse	Using a network connection to execute malicious code	This threat group refers to gaining complete or partial remote control of the devices. It ranges from remote command execution using one device to organizing nets of smart devices for executing a particular action – botnets. An example of a botnet attack based on smart device resources is a DDoS attack launched with the help of hacked devices connected to HANs. The authors of the attack could make use of the factory-set default usernames and passwords to take control over devices and then force them to generate artificial traffic, which would heavily load selected DNS servers.[18]
	Denial of service	The main risks arising from the use of constrained devices in the Smart Home environment is their vulnerability to DoS attacks, which might lead to the rapid exhaustion of constrained node resources. Typically, the limited CPU and memory resources mean that constrained devices are vulnerable to resource exhaustion attacks [29]. It provides an opportunity for the attacker to send requests continuously, which will be processed by some nodes causing resources overutilization. Furthermore, it results in congestion in radio channels, which finally could result in disabling communication channels between smart objects. Zorzi et al. [30] observed that using large traffic volumes on radio channels to flood the network could also forcibly disrupt the network availability, even in the case of requests without responses. Moreover, this kind of attack exploits vulnerabilities of IoT protocols implementations, where one of the illustrious examples is the ZigBee radio technology. Though the ZigBee standard assumes different security mechanisms, many stack implementations include only basic security services which do not ensure safe communications. Example vulnerabilities are presented in the Cognosec report [20]. Zillner outlines that (for implementations with reduced security mechanisms) encryption keys are often transmitted in an unencrypted format when a new ZigBee device joins HAN. The DoS attacks might be directed against nodes engaged in communication on the end-to-end path [31]. In this context, DoS attacks might cause service unavailability, i.e., unavailability of web portals used to control HAN devices.

(Continued)

[18] https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.

Table 3. Continued

Threats category	Threats	Characteristcs/ attack examples
	Unauthorized access to the local network resources	This group of threats is associated with access to HAN-connected devices, and specifically settings which might influence their network communication. This group of threats was outlined by the Open Web Application Security Project (OWASP)[19] as follows: • Insecure Network Services, which may be exploited to disable devices connected to HAN; • Insecure Software/Firmware, which could give access to the potential attacker for performing her/hisown malicious update, e.g., via DNS hijacking; and • Lack of Transport Encryption/Integrity Verification, which may result in eavesdropping of data being passed over HAN. The above threats include also poorly secured end-to-end transport services implemented in some smart devices. The OWASP also highlights security flaws in management functions and particularly web application security.
Dependability and reliability	Outages/ Disasters affecting Internet connection	This threat category extends the cases specified for perceptual layer and refers to resources accessible over the Internet. Exemplary attacks may cause outage of Internet access, which is required by some smart home applications.
	Failures/ Malfunctions affecting Internet connection	This threat category refers to failures and disruptions of service providers at the network level.

The starting point for ensuring the confidentiality in IoT systems is a set of adequate standard mechanisms used in current IT systems such as: AES for encryption of data transport, RSA for public key encryption, and digital signatures and DH protocol for shared key agreement and management. The above-mentioned tools can solve a majority of the problems of IT systems security and the experience gained from their application significantly influenced recommendations on the use of specific variants of those tools. One of the good examples of such recommendation is the document issued by the National Institute of Standards (NIST) [34]. Barker and Roginsky point out that at least a 128-bit key strength encoding is required for most of the current used IT applications. According to this recommendation, shorter keys may also be applied but the frequent key replacement is required to undermine the compromising communications between two legitimate peers. Currently, AES-128 is the *de facto* standard to ensure confidentiality/privacy and is adopted by many HAN communication standards (i.e., BLE, Z-Wave, ZigBee, EnOcean, etc.).

The most commonly used security protocols within HAN and WAN provide similar functionalities but at different layers (i.e., the TLS/SSL is a protocol suite for link encryption at the transport layer while IPSec is a protocol suite running at the networking layer). However, computation overhead related to implementation of such protocols often eliminates them from using in constrained networks. Instead, solutions based on DTLS [35] (UDP equivalent to TLS) may be exploited. The

[19] https://www.owasp.org.

Table 4. Threats at the Application Layer

Threats category	Threats	Characteristcs/ attack examples
Nefarious Activity/Abuse	Denial of Smart Home service	At the application layer, DoS attacks might be directed toward particular services that are used by the smart home solutions vendor (i.e., new devices registration). The attacks may be performed by overloading servers with requests, thus causing HAN management systems to be unavailable.
	Compromising confidential information and abuse of personal data	This group of attacks is directed toward the cloud service provider and IoT solution providers that store the user's data from smart home applications. Cloud providers are treated by users (and smart device manufacturers) as the trusted partner and let them store large amounts of sensitive data (i.e., cloud-based home monitoring, etc.). Some example attacks are explained in detail in [32]. The Smart Home data stored in the vendor's cloud is also susceptible to malicious insider attacks. These data might be illegally accessed by a rouge employee and used either to violate a device owner's privacy directly or as part of a larger data breach, especially when, e.g., using default credentials in appliances.
	Unauthorized access to information system/network Unauthorized use of administration of devices & systems Abuse of authorizations	This group of threats is associated with access to management functions and particularly is critical to web application security. Flaws in this area has been also broadly discussed by OWASP. The most outstanding conclusions are about the potential attacks to surface areas. From these, a number of vulnerabilities could be summarized as follows: • Insecure Web Interface, which may be exploited by as attacker if weak or no credentials are used (e.g., plain text for transmitted passwords); • Insufficient Authentication/Authorization, which may be exploited by an attacker in case of weak passwords, insecure password recovery mechanisms or lack of granularity in access control in order to access a particular interface; • Scarce Personal Data Protection, which increases the privacy concern; • Insufficient Security Configurability caused by lack of granular permissions to access the data or control the devices; • Insecure Mobile Interface, which may be exploited by a potential attacker to access data or take control over HAN devices via the mobile interface;

(Continued)

Table 4. Continued

Threats category	Threats	Characteristcs/ attack examples
		• Insecure cloud interface may be exploited by a potential attacker who wants to access data or smart device management via the cloud API. The above list suggests that, except the human factor, typical vulnerabilities are related to insufficient protection of API mechanisms on different transmission layers, but in particular at the application layer. The above list of vulnerabilities remains valid for different levels of access, i.e., direct-access smart device's built-in web server, home gateway or even cloud-based control panel. Security analysts point out that application frameworks based on cloud services for smart device management might not guarantee also acceptable security level. Some example security flaws resulting from overprivileged applications were described in [33].
Dependability and reliability	Outages/Disasters Damage/Loss of IT assets	This threat group extends cases specified for perceptual and network layers and refers to service specific resources accessible over the Internet. Exemplary threats may encompass unavailability of specific services required by smart home applications (i.e., device vendor support servers).

TLS protocol is used in the IoT architectures and protocols based on TCP, such as MQTT [36] or SmartM2M[20] standardized by ETSI, while DTLS is used by protocols that rely on UDP for its transport layer, as OMA LightweightM2M (LWM2M)[21] that uses CoAP [37]. However, the TLS is still used when accessing the cloud-based Smart Home applications (i.e., Apples HomeKit, which uses, for this purpose, the HTTP secured using TLS with AES-128 bit key).

Particularly in context of the IoT, the DTLS protocol is still a subject to improve in many research activities. For example, Keoh et al. [38] proposes optimizing the DTLS communication protocol for securing IoT data exchange by reducing complexity, Altolini et al. [39] advises the implementations of IEEE 802.15.4 to be compliant link-layer security procedures, and Wen et al. [40] presents a lightweight encryption/decryption method for authentication purposes in constrained network. Some security concepts related to Smart Grids assume also specific methods for secure information aggregation. In this context, Li et al. [5] proposed a solution which makes use of homomorphic encryption. It enables transmitted data (meter readings) to be aggregated without being decrypted at the packet level.

It was widely accepted that software implementation of constrained devices does not exploit extensively the PKC because of overheads related to large key sizes. For instance, such thesis is

[20] ETSI SmartM2M provides specifications for M2M services and applications, focusing on aspects of the IoT aspects and Smart Cities (http://www.etsi.org/technologies-clusters/technologies/internet-of-things).
[21] OMA LightweightM2M (LWM2M) is an industry standard for device management of M2M/IoT devices. It relies on CoAP protocol and therefore is optimized for communications over sensor or cellular networks.

presented in [41] and [42]. The remedy for that aimed at (1) securing transmission only between selected (relatively less constrained) nodes across the network and (2) applying less resource consuming encryption methods for constrained devices. The first objective may be achieved by running good practices (see Section 6 for details) avoiding communication directly with constrained nodes, whereas the second objective may be fulfilled by using one of the public keys encryption algorithms suitable for communicating constrained nodes: Rabin's Scheme [43], NtruEncrypt [44] and Elliptic Curve Cryptography (ECC) [45]. The above-mentioned algorithms have been validated many times on popular developers' sensor nodes. Researchers proved that applying these algorithms may result in satisfactory transmission effectiveness while consuming relatively limited physical resources. However, the problem is in the selection of appropriate parameters to optimize the encryption design. As shown in the literature (i.e., [46]), higher simplicity offers faster encryption and decryption processes in ECC cryptography compared with the RSA cryptography. Therefore, ECC-based cryptosystems are interesting for use by IoT objects due to both the reduction of processing and communication overheads [47].

At last, let us remark that research results proving that the PKC algorithms could be used in WSNs have been presented in [48] and in [49], but their implementation in HAN has not been demonstrated yet. Most of the key management protocols for wireless sensor networks are probabilistic and distributed schemes. They exploit various methods for generating and distributing the keys which remain unchanged during the session. It has the advantage of lower power consumption compared to the dynamic keying. The greatest contribution to this work may be found in [50] and [51]. Further research work has been focused on improving these methods.

5.2 Integrity

Typically, in IT systems, ensuring the integrity can be achieved by the content digest calculation and appending them to the transmitted content. In WSNs digests are usually generated using hashing algorithms like SHA [52]. Typical sizes for these digests (so called the SHA-2 family) are: SHA-224, SHA-256, SHA-384, and SHA-512. Current research efforts in this area are being provided by the National Institute of Standards and Technology (NIST), among others; NIST initiative has chosen the compact Secure Hash Algorithm SHA-3 as the new algorithm family for the so-called "embedded" or smart devices. These devices connect to electronic networks but are not themselves computers. However, other hashing functions including the SHA-2 still remain secure according to the NIST.

These variants represent an iterative cryptographic hash function which does not contain a secret key. However, if digest generation involves a secret key, then the hashing function algorithm requires adaptation. The examples of such modified algorithms are keyed-hashing functions for message authentication (HMAC), but only a subset of them can be used on constrained platforms because of poor performance optimization. A good example is the CMAC algorithm proposed in EnOcean standard. The modified algorithms designed to work with keys are mostly the same as for ensuring the authenticity. The 802.15.4/ZigBee and BLE (ver. 4.2 and higher) series of standards introduced combination of an AES-128 encryption in counter mode and a Cipher Block Chaining MAC (CBC-MAC). For the same purpose, the Z-Wave operable devices make use of the pure CBC-MAC code (it is implemented starting with the 400 series chips).

An alternative approach, which aims to check whether received data is trustworthy, is its correlation with historical data. For example, Przydatek et al. [53] proposes a solution assuming that the home server (which aggregates measured data from remote sensors) checks whether the reported result is "close" to the expected aggregated value. If the reported value is significantly different from the expected one, then the home server might decide to reject the received data and label it as corrupted or compromised. Consequently, adequate decisions would be taken in relation to the node that sent this data.

Integrity tampering is not limited only to message modification but also encompasses malicious data injection attacks or replay attacks. In this regard, literature analysis reveals that limited resources of particular HAN nodes imposes real limits on the possible cryptographic techniques. Threats and countermeasures for HAN nodes are analyzed in [54], where lightweight digital watermarking technique is also proposed. Authors prove its usefulness as protection technique for real-time intelligent meters data. Another method for false data and replay attacks detection has been proposed in [55]. Huang et al. [55] described a new approach to the defense strategy against specific attacks that are typical in Smart Grids. The main goal for such strategy is to detect changes in statistical behavior as quickly as possible. Detection algorithms proposed for this strategy are based on real-time observations of transmitted data. The authors chose non-Bayesian framework, specifically the so called cumulative sum -CUSUM- test. The proposed test procedure is based on checking the characteristics of data distributions at random times. According to the authors, the CUSUM test is an effective tool for quick intrusion detection in real-time processes. Moreover, it requires a minimum number of observations to detect an attack with a relatively high probability.

Apart from the above-mentioned tools for integrity violation detection, adequate countermeasures for unauthorized modifications should also be addressed. Therefore, the use of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in HAN deployments is extended in commercial devices. The question arising for adopting IDS/IPS to Smart Home is their ability to analyze the behavior of constrained node activity. Further, on that basis, the comparison between current and normal system behaviors should be performed. By the term *normal behavior*, we mean the functioning of the system without intrusions [56]. This idea inherited from Artificial Immune System (AIS) concept was presented in literature by [57] and [58], where the authors presented a set of algorithms aimed to detect attacks on IoT devices and defend against them.

5.3 Authentication and Non-Repudiation

The HAN nodes authentication is mainly based on cryptographic techniques used for ensuring integrity. A classic technique makes use of MAC, which uses a secret key to encrypt hash of the content message. Fouda et al. [59] proposed MAC-based mechanism dedicated for meters data gathering within the Smart Grid infrastructure. A slight modification has been proposed in [60]. This solution proposes a variable MAC for authentication between the group of AMI (Advanced Metering Infrastructure) devices and the control nodes. Other solutions proposed methods that exploit hash functions [61]. The hash-based and MAC-based authentication methods rely on both types of cryptography (Public and Private Key Cryptography) and make use of standard key distribution methods and protocols.

Robust protocols require high processing overhead that may not be supported by all IoT-attached devices. Consequently, authentication requires appropriate reengineering to adapt to Smart Home needs. Authentication has been adapted for different IoT hardware platforms such as AES/RSA [62] for Bluetooth devices or 802.15.4/ZigBee radio.[22] The standard approach in this case assumes that all the constrained nodes within the network use a common pre-shared key. This solution is sufficient in the case when we want to protect access via controller to HAN. In this context, the Z-Wave technology enforces that messages are signed by generated MAC code in the CBC mode of AES. As mentioned earlier, this is possible starting with series 400 of Z-Wave chip. The 802.15.4/ZigBee and BLE (ver. 4.2 and higher) standards offer the CBC-MAC (CCM) mode of encryption – the combination of CBC-MAC mode and the counter mode. An alternative authentication scheme CMAC

[22] http://www.libelium.com/products/waspmote/encryption/.

(MACs based on block ciphers) is also used for guaranteeing the non-repudiation of exchanged data in EnOcean network.

Another approach to the non-repudiation guaranteeing is presented in [63]. It assumes that each subscriber's smart meter has its counterpart (in neighborhood) representing the providers reading. The readings on both meters are usually not equal because of energy loses but their higher inconsistency may suggest communicating node compromising. In this context, the mutual inspection procedure helps to ensure that exchanged smart meter readings are received from the right sender. This method is also representative for non-repudiation mechanisms, which are based on data trends analysis; however, in this case, the requirements of storage and CPU usage are high and the method cannot be applied by constrained devices.

Cryptographically digital signatures are used also for protecting transmitted raw data. In this context, it becomes important to point out the procedure describing how the message content is prepared to be used by a cryptographic algorithm. It is desirable that the cryptographic mechanism should be adjusted to fit the structure of the data, which the algorithm aims to protect. An example of implementation of that structure is the one based on the Javascript Object Notation (JSON), which has recently become very popular to represent data in the IoT domain (and not only) [64]. Taking into consideration the JSON notation, one of the candidates to sign structured data is the JSON Web Signature (JWS) which ensures content security with digital signatures or MACs [65].

5.4 Availability

5.4.1 Physical Protection. The HAN needs to create tamper resistance into devices so that the environment is resistant to extraction of sensitive information like personal data, cryptographic keys, or credentials. Finally, it is expected that IoT devices will have long life-cycles, so it is important to enable software updates to properly exploit the devices after their release.

Taking the risks related to every-day smart device exploitation into consideration, organizational solutions that support security should also be applied. Basically, we can identify two key ways for organizational solutions that allow the achievement of Smart Home deployment security:

- The first one assumes engaging a network operator to become the preferred trusted third party. In this case, it would be responsible for supplying and maintenance of dedicated (proprietary or nonproprietary) home gateway.
- The alternative way assumes that Smart Home control functions would be performed by applications supplied by smart appliance manufacturers. In this case, suppliers would be responsible for implementing control/monitoring applications as well as drivers for their technologies which would be able to run on such universal home gateways.

The combined approach has been outlined by Volner et al. [66]. They presented a concept of the universal open HG, maintained by a service provider. According to this idea, the HG would offer well-defined interfaces open to the smart devices. This approach is an open research issue, which could provide not only availability of the system, but also could improve management and control of the Smart Home together with easy security and privacy updates in the environment. This issue will be extensively described in Section 6.

5.4.2 Access Control. The HAN security may also suffer from constrained access control that may be caused by wireless connection instability, which makes it impossible to modify the access control rules. It often results from local conditions that influence in turn the propagation conditions. Even the short-term wireless connection outages can make smart devices unprotected and liable to attacks. The connected smart bulb, bathroom scale, and door lock may become the entry to take over the control of other constrained nodes within the HAN. Also subjugating access control settings without wizards and manuals is a difficult task, especially for non-professionals. Moreover, Smart Home deployments are usually heterogeneous environments that must consider the diverse needs and habits of the household inhabitants. On the other hand, limited resources of smart objects do not allow the implementation of advanced access control mechanisms. For this reason, current access-control systems dedicated to constrained devices handle partial exceptions and various levels of user rights [67]. Moreover, many market-available solutions assume trust relationships between HAN users (family members, neighbors, guests, etc.); however, they usually do not consider the installations, which are shared among local (neighbor) community like, e.g., surveillance systems in nearby houses [68].

In conclusion, availability issues may and should be solved through up-to-date mechanisms installed in both constrained and powerful devices. The barrier is who is able to update security software in home environment for an extended public. This issue will be discussed in Section 6.

5.5 Authorization

One of the common authorization solutions used in IT systems is the use of Access Control List (ACL). This method adopted for use in Smart Grids has been presented in [69] but the CPU requirements to the meters (constrained devices) are too high and due to this fact, no solutions have been implemented with this technique. There are relatively few lightweight authorization solutions [15] that could be used in Smart Home environment. One of them, presented in [70], proposes an authentication mechanism that exploits policy-based access control scheme and uses central Key Distribution Center (KDC). This solution requires that one entity in HAN has online access to KDC, what makes this entity vulnerable to attacks. This drawback has been eliminated in distributed authorization system presented in [71]. The authors proposed a distributed mechanism that performs access control tasks and, in addition to this, it is responsible for data aggregation. Gathered data are encrypted using a set of parameters before sending them to the central repository (parameters may be any information related to data). Another encryption method related to access control has been proposed in [72]. Wu et al. [72] defined a new system which differentiates access rights in detail and applies assigned rules to protect data transmission over the radio link. This scheme makes use of a cryptographic mechanism referred to as Fuzzy identity-based encryption with dedicated error-correction coding.

Studies in this field were also performed within the SMARTIE project, where several authorization enablers (targeting several use cases) were proposed for constrained sensors and powerful devices as well. They make use of a lightweight version of Extensible Authentication Protocol over LAN (EAPOL) to initiate authentication process from the authenticator (server) side in which the server asks connected device to verify itself. Moreover, this protocol allows also to use RADIUS (Remote Authentication Dial In User Service) authentication. Further on, the authors have also added support for Extensible Access Control Markup Language (XACML), which is the general-purpose access control policy language.

Also SmartHG project dealt with authorization mechanisms and proposed a new encryptation method for constrained devices. It applies the EEC encryption to paired devices, which are intended to join the so-called "Trust Domain" [73]. For this purpose, the proposed method makes use of a bootstrapping protocol that serves the exchange of device IDs to establish key-pairs, which will be further used during communication within the Trust Domain. An interesting approach is that, depending on security policies, the keys could not be stored at all or they could be stored only for a short time. Obviously, the key may be permanent for fully trusted devices and may be also acquired from external servers. In the authorization context, the proposed SmartHG solution supports a Smart Home's Trusted Domain containing distributed software (running in HG) that is responsible for tracking on the Internet the devices which joined the HAN [74]. Then, the Trusted Domain consists of devices linked together by the user in conscious manner (such as smartphones, tablets, game consoles, etc.). During the linking process, the devices perform the procedure of tokens exchange. As a result, both sides trust each other while joining the Trusted Domain. On the other hand, the HG protects constrained devices within HAN from access from the Internet and prevents from leaking private data.

5.6 Implementation Issues

5.6.1 Hardware Limitations. There are many factors that determine whether it is feasible and cost effective to implement given security mechanisms in smart devices. Literature examples point out that the most important factors determining the choose of the proper secure communication are available throughput, bandwidth and latency [18]. Moreover, an important limitation, aside from device capabilities, is also environmental conditions which influence, e.g., radio wave propagation. Therefore, a choice of the proper security suite is a compromise between reliable transmission, possible attack consequences and ease of use. Following the RFC7228 document, constrained devices can be classified into three categories based on their computation ability, memory/storage, and available energy supply. These categories are shortly characterized in Table 5 together with the possible security suites.

The above classification takes into account commercial use of smart devices and does not include non-commercial solutions, which are implemented on development boards.

Another criteria taken for constrained devices classification is availability of energy for the operation. Following the RFC7228 document, constrained devices are divided into following categories:

- *E0 (Event Energy-Limited).* The device has the amount of energy that is sufficient to handle a single event (Event-based harvesting);
- *E1: (Period Energy-Limited).* The available energy is limited to a specific period (e.g., Battery that is periodically recharged or replaced);
- *E2: (Lifetime Energy-Limited).* The device has a total energy limit over its usable lifetime (e.g., Non-replaceable primary battery);
- *E9: (No Direct Quantitative Limitations to Available Energy).* Energy source is unlimited in availability (e.g., mains-powered devices).

According to the above classification, only devices from the E9 have enough energy to serve security mechanisms (i.e., payload data encryption). Due to its specificity, devices classified as E0 do not perform tasks that require secure communication. In case of devices classified as E2 and E9, security mechanisms can be implemented considering energy consumption in computation of the security functions. In specific embodiments, other factors need to be considered, i.e., desired level of security, usability, and profitability of the solution, and the like.

5.6.2 Support for Secure Communication with Cloud Platforms. As stated before, many smart home applications exploit mobile devices for control of the home's systems over HAN. Usually, they use vendor's (or 3rd party) cloud services for management function instantiation. This requires secure communication among the smart device, the cloud infrastructure, and the mobile phone. Analyzing currently available IoT Cloud Platforms, we can observe that this communication is mostly established by using session security based on TLS. Certificates where TLS is used are server authentication (Microsoft Azure IoT Hub[23]) and two-way authentication (AWS IoT[24]). The

[23] https://azure.microsoft.com/en-us/services/iot-hub/.

[24] https://aws.amazon.com/documentation/iot/.

Table 5. Hardware Limitation Classes According to RFC7228

Smart device Class	Available RAM size	Data storage size (e.g., flash memory)	Characteristics and security mechanisms implementation
Class 0 (C0)	$\ll$10 kB	$\ll$100 kB	Objects need an intermediary support (acting as gateways, or hubs) for transmission over the Internet because of substantial hardware limitation and possible battery drainage. Usually, they do not implement security mechanisms in terms of payload data encryption. Examples are simple sensors and meters. However, there are also devices that basically fall into this category but offer parameters close to the C1. As far as (radio) transmission conditions allow, vendors implement secure data communication between the device and intermediary node based on a 128-bit symmetric encryption (AES-128).
Class 1 (C1)	~10 kB	~100 kB	Devices with limited memory size and computational performance which usually make the implementation's full IP communication stack unavailable. However, essentially battery supply is not a limitation in this case. Therefore, lightweight versions of secure transport mechanisms can be implemented if End-to-End secure transmission is required. For that purpose, the most popular DTLS is often used. Due to high resource requirements (memory and computational capacities), the two-way authentication process can be performed using ECC. Moreover, they can make use of pre-shared key for ECC.[25]
Class 2 (C2)	~50 kB	~250 kB	This category includes devices which are essentially able to perform point-to-point data exchange over the Internet. For security reasons they can make use of the DTLS protocol with ECC authentication. If PKC is required, vendors also should be able to implement support for the X.509 certificates.

set of authentication methods encompasses X.509 certificates (for advanced devices/hubs) SHA-1/SHA-2 based certificates (for constrained devices) or proprietary identification methods (i.e., ID devices groups in AWS IoT).

[25] https://tools.ietf.org/html/draft-schmitt-ace-twowayauth-for-iot-02.

At the application layer, all platforms offer HTTP protocol, however additional protocols for data exchange like MQTT (i.e., Xively,[26] AWS IoT), AMQP (i.e., Microsoft Azure IoT Hub) or CoAP (i.e., Samsung Artik Cloud[27]) are also broadly used.

6 GOOD PRACTICES

6.1 General Approach

One of the results of the research provided in Secure Smart Homes is that the security tasks should be as light as possible during installation and exploitation. Therefore, suppliers may preconfigure their equipment or introduce simplified security procedures if constrained devices are interworking in homogenous environment (i.e., all devices from one supplier). On the other hand, the Smart Home environment should take into account comprehensively all the above-mentioned security aspects. To reconcile the expectations of users and suppliers, a number of "good practices" should be considered by all the stakeholders in order to mitigate the threats analyzed and identified in Smart Home environment [1]. These good practices should go from basic security hygiene to dedicated countermeasures against given types of threats, for different types and classes of devices as well as for associated remote services. Common guidelines for users, software and hardware developers are categorized as follows:

- Security audits, which means that security events logging must be enabled, and the users should be notified when required. It also encompasses prevention of these data from unauthorized access;
- Protecting of communications within HAN and WAN, which includes protecting against message removing, modification, disruption or cloning as well as against DoS attacks;
- Ensuring confidentiality, integrity, and authenticity by using strong standardized cryptography methods, where in cryptographic keys are managed securely, and the use of a trust infrastructure (such as PKI) is encouraged;
- User data protection, which encompasses the integrity, confidentiality and authenticity of user data;
- Authentication and authorization, which assume strong methods for authentication, authorization, and identification and also involve access control mechanisms;
- Hardware and software self-protection, which should be installed to gain protection of the above-mentioned security features and to reduce the attack surface.

Applying these guidelines should not significantly hinder the use of Smart Home devices.

Good practices for security purposes assume two scenarios: the first one is a homogeneous scenario where one vendor supplies all the devices and software. The second scenario is when the consumers integrate a number of devices or small systems and configure the elements by their own (e.g., smart light bulbs). The first scenario assumes that data transmission is performed via dedicated controller (e.g., ZigBee, Bluetooth) or directly via the WiFi enabled gateway. However, the devices are allowed to connect to the Internet in order to maintain cloud maintained services provided by the vendor of the devices. Such solutions are quite extended, as pointed out in the report [75] and encompass popular radio technologies such as Z-Wave (e.g., Fibaro motion sensor [76]) or ZigBee.

In homogeneous scenario, the credentials are provisioned by the hardware manufacturer in a similar way as they are provided WPANs, where key distribution uses predefined keys.

[26] https://www.xively.com/xively-iot-platform.
[27] https://artik.cloud/.

In heterogeneous scenarios, security is more compromised and, for this reason, devices have to be delivered pre-installed to some extent. However, the suppliers should be aware that a user who has to spend much more time on securing a smart object, she/he will likely abandon such action. Therefore, Smart Home (components) should be provided with tools, which simplify the configuration and exploitation security installation process.

In this case, the authorization solutions differ between concepts of the Smart Home. For Smart Home typical scenarios, the solutions include setting up the pin code or password when accessing the HAN or when pairing two devices for communication. For large-scale deployments typical for enterprise applications, this operation is automated. In this case, a standard procedure assumes the use of mobile cellular networks because of their global coverage and their capacity of to handling a large volume of traffic.

6.2 Securing Communication for IoT/M2M Cloud Platforms

The communication of HAN with the Internet is always more used for Smart Home management. On the one hand, the devices are increasingly responsible for collecting and transmitting sensitive information to the cloud. On the other hand, manufacturers control the life-cycle of the devices through the Internet connection. At last, users want to manage the devices from anywhere using various end devices (i.e., smartphones, tablets, dashboards, etc.). Connected (directly or indirectly) smart devices and mobile applications must be authenticated on the platform. Both the mobile application and the end user's credentials must pass authorization.

Due to the diversity of applications making use of the HAN-cloud communication, the necessity of new standards for end-to-end encryption has arisen. Several standards ensure the confidential transmissions from devices to mobile applications and to clouds. These standards are also used by cloud-based integrated Smart Home systems, which create devices with secure communication while allowing the applicability of the devices to the consumers. The Google's Nest platform[28] contains a set of smart devices using Nest cloud services over Internet connection. It makes use of different encryption mechanisms. Essentially, the control application and Nest devices (i.e., Net thermostat) connect to the Nest cloud service over the TLS connection encrypted with the AES 128. Moreover, CO and smoke sensors (Nest Protect devices) use a proprietary secure protocol similar to TLS for sharing data. Finally the Nest-capable camera (Nest Cam) uses 2048-bit RSA keys for a key exchange, and then encrypts the streaming transmission using the obtained AES-128 key.

The Apple's HomeKit is a new network protocol that allows users to control home appliances or to access certain services. It offers integration of diversity of applications into a smartphone and allows to group resources based on common features. Secure pairing of devices ensures to the users that they are the only persons controlling the device. HomeKit enforces encryption between the iOS device and the accessories by using public-private key pairs. The pairing process between an iOS device and a HomeKit device is performed by using Secure Remote Password protocol. This protocol performs exchange of information about paired devices identified by an 8-digit code permanently assigned to the constrained device by the iOS device user. Then, obtained data are transmitted over encrypted link using ChaCha20-Poly1305 AEAD, which is an operation secured with HKDF-SHA-512-derived keys. The ChaCha20-Poly1305 AEAD is a composition of the ChaCha20 stream cipher and the Poly1305 polynomial MAC for message authentication. Both operations form one security mechanism called AEAD (Authenticated Encryption with Associated Data). This mechanism is specified for use in TLS as specified in [77].

[28] https://nest.com/support/.

Similar to these solutions, AllJoyn[29] implements security mechanism at application level, therefore there is no trusted connection being realized at lower levels. In the moment when a new device tries to connect, an authentication demand is triggered between the applications. This action supports multiple algorithms like PIN codes, PSK or Elliptical Curve Digital Signature Algorithm (ECDSA). After completion of the authentication phase, the transmission is encrypted using the AES-128 block cipher in Counter with CBC-MAC (CCM) mode.

7 OPEN RESEARCH ISSUES

The development of Smart Homes is bringing a number of challenges not only in security and privacy but also in the general management of HANs. Among the new requirements for HAN managements, we may outline the following: remote access and ubiquitous management, interoperability with increasing 3rd party IoT services developers and increasing demand also for inexpert users. Therefore, an efficient intercommunication platform for Smart Homes should be deployed. Such a platform should be extendable, easily manageable, secure with different levels of privacy and security, open to interoperability, and robust.

The exposed necessities show that this platform should be managed by an external actor, which is trustful for the end users and is able to control and maintain the management layer of the HANs (including security) without the necessity of active engagement of the end users. The actor who is best positioned to manage HANs is the network operator (to which HAN would be attached). Currently, network operators are going into the houses through the management of multimedia services and, concretely, through the management of set-top-boxes offering all kinds of multimedia content (VoD, IPTV, interactive TV…). Extending the functionalities of set-top-boxes does not seem to be a difficult task for network operators. This means that the potential and new business models of introducing management of HANs seem to be very large.

Technically, two elements are necessary for creating this easy-to-use, secure, and fully managed Home Automation Network: the Multi-Functional Home Gateway (MFHG) and the HAN Management System (HMS).

On the one hand, MFHG is an intelligent device owned by the network operator and located in the user's house. The MFHG fulfills functionalities of multimedia distribution in the house (set-top-box operations for the control of Home Area Media Network) in addition to router functionalities and will also manage the Home Automation Networks at the end-user's premises. The MFHG will connect the HAN with other remote machines. Such a communication will be based on unified Application Programming Interface (API), which translates the instructions to the devices of the HAN by mapping the unified API to the vendor API (the API of the constrained and powerful devices defined by the vendor of the device). The main goal of the unified API is to build a homogeneous environment for IoT services using different resources. This way, even if the IoT services are composed on different functional domains (i.e., smart city, intelligent home) with different formats, the service developer may access to them via common interface. As a result, the service developer can be unaware of network technology used by particular objects and device constraints and the services are easily portable between HANs. It will allow a user to run locally created custom application (i.e., for intelligent building, etc.) and share the application to other users owning similar but not the same devices. In other words, thanks to the use of unified API, the IoT becomes ubiquitous, which makes feasible the integration of different spheres of IoT into the same application.

The MFHG will be fully managed by the network operator, which will maintain up-to-date software containing new vendor APIs (and respective unified API instructions) and assuring all

[29] https://allseenalliance.org/.

levels of security based on trustful identities of the elements (e.g., mobile phone, cloud managers, etc.) requiring access to the HAN. Moreover, the MFHG managed by the operator is in charge of assuring privacy of data stored in the HAN.

On the other hand, a management system called HAN Management System (HMS) will be deployed at network operator's premises and will fulfil tasks of MFHG management. HMS main functionality is to update security mechanisms into the MFHG in order that the MFHG will make the communication of the HAN with external elements feasible through different security levels on dependence of the identity of the external elements. Security software will be updated into the MFHG (process triggered and managed by the HMS) and new identities uploaded, if needed. The communication between HMS and MFHG will be ensured with the highest levels of security in configuration phase.

Moreover, HMS will be responsible of maintaining up-to-date software for connecting to vendors' devices as well as making the objects accessible from outdoors (unified API). Once again, through continuous software updates, the network provider will ensure that new HAN equipment created by vendors may be easily incorporated to the HAN and may be connected through unified API. The MFHG will be in charge of automatically connecting plug-and-play objects and registering them together with the potential services offered by the objects, whenever a previous agreement will be reached between HMS and device vendors for updating APIs.

3rd part IoT service sharing platform (e.g., Xively) will be directly contacted by the management system in order to adapt IoT services (created by 3rd part users) to unified API access. This functionality has sense in the spectrum of unified APIs of all the IoT services. Also the services created in the HAN may be shared in a public sharing platform installed in the Network operator management system.

Figure 3 shows the relations between the HMS, MFHG, and other external elements. The users (e.g., the owner of the HAN from her/his own mobile cell), which want to have access to the HAN, must contact earlier with the HMS to contract the desired security level and access to the HAN functionalities (creation of identity). Once the security level and Authorization and Authentication procedures have been agreed, then the users may directly contact the MFHG (validation of identity). The MHFG will be aware (through the communication with the HMS) about Authorization level and Authentication procedure for giving access to the user.

The middleware level will introduce several levels of security related to different potential identities with access to HAN (behind MFHG). Therefore, different levels of security could be created based on credentials considered secure in several Internet scopes. For example, credentials as Facebook access could be a valid identity and would have assigned a number of permissions for such an identity. Logically, the permissions assigned to this identity will be much more limited than the ones assigned to an identity confirmed by tokens or other secure systems in the MHS.

Given the fluid nature of identity in the HAN, understanding and management of trust becomes important. Devices may be replaced frequently (e.g., cell phones), relationships may be ephemeral (e.g., a purchase from a vending machine), and trust can have transitivity (as when devices owned by friends are also to be trusted). Webs of trust will become more complex and many more levels of trust within communities may be required. Therefore, we think that the cooperation between the end-users and the network operator may be crucial in the case of evolving reality. The end-user is not able to follow the communities, the legal entities which may require access to the HAN and, on the other side, the network operator is unaware of the user's relationships. Therefore, the operator and the user together will be responsible for the safety of all the outside-in and inside-out communications.

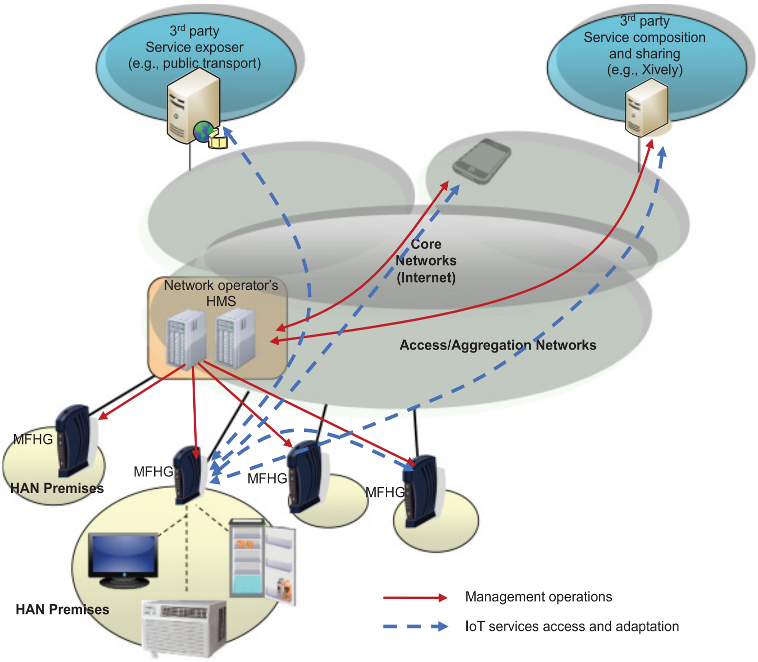

Fig. 3. Future HAN managed by Network operator.

8 CONCLUSIONS

This article discusses the issues of security in Smart Home systems and proposes future scenarios for tackling all the challenges inherited from the development of Smart Homes related to security, privacy, as well as manageability.

For security aspects, we presented an extensive overlook of the proposed solutions ordering by complexity, use spreading, interoperability and efficiency. We considered all the areas of security where Smart Homes are threatened, i.e., confidentiality/privacy, integrity, authenticity, non-repudiation, availability and authorization, and discussed about the valid and invalid solutions for current systems integrated into the home environment. The conclusion is that the Smart Home are vulnerable in several points and a secure management system should be integrated to the Smart Homes. We argued that it is necessary to introduce external actors capable of managing the system introducing security in all layers and ensuring privacy of data, and pointed out that the network operators are the best positioned to give management support to Smart Homes since they are already present in the houses through home gateways for multimedia delivery.

REFERENCES

[1] Cédric Lévy-Bencheton, Eleni Darra, Guillaume Tétu, Guillaume Dufay, and Mouhannad Alattar. 2015. Security and resilience of smart home environments good practices and recommendations. Tech. Rep. European Union Agency for Network and Information Security.

[2] Karsten Bormann, Mehmet Ersue, and Ari Keranen. 2014. RFC 7228, Terminology for constrained-node networks. Retrieved July 10, 2017 from: https://tools.ietf.org/html/rfc7228.

[3] Federico Viani, Fabrizio Robol, Alessandro Polo, Paolo Rocca, Giacomo Oliveri, and Andrea Massa. 2013. Wireless architectures for heterogeneous sensing in smart home applications: Concepts and real implementation. *Proc. IEEE* 101 (2013), 2381–2396. DOI: https://doi.org/10.1109/JPROC.2013.2266858

[4] Tianming Li, Narayan B. Mandayam, and Alex Reznik. 2013. A framework for distributed resource allocation and admission control in a cognitive digital home. *IEEE Trans. Wireless Commun.* 12, 3 (2013), 984–995. DOI: https://doi.org/10.1109/TWC.2012.011513.111495

[5] Tongtong Li, Jian Ren, and Xiaochen Tang. 2012. Secure wireless monitoring and control systems for smart grid and smart home. *IEEE Wirel. Commun.* 19, 3 (2012), 66–73. DOI: https://doi.org/10.1109/MWC.2012.6231161

[6] Prafulla N. Dawadi, Diane J. Cook, and Maureen Schmitter-Edgecombe. 2013. Automated cognitive health assessment using smart home monitoring of complex tasks. *IEEE Trans. Syst., Man, Cybernet,: Syst.* 43, 6 (2013), 1302–1313. DOI: https://doi.org/10.1109/TSMC.2013.2252338

[7] Juan A. Nazabal, Francisco J. Falcone, Carlos Fernandez-Valdivielso, and Ignacio R. Matias. 2013. Energy management system proposal for efficient smart homes. In *Proceedings of the 2013 International Conference on New Concepts in Smart Cities: Fostering Public and Private Alliances (SmartMILE).* DOI: https://doi.org/10.1109/SmartMILE.2013.6708174

[8] Meg E. Morris, Brooke Adair, Kimberly Miller, Elizabeth Ozanne, Ralph Hansen, Alan J. Pearce, Nick Santamaria, Luan Viegas, Maureen Long, and Catherine M. Said. 2013. Smart-home technologies to assist older people to live well at Home. *J. Aging Sci.* 1, 101 (2013). DOI: http://dx.doi.org/10.4172/2329-8847.1000101

[9] Katherine Wild, Linda Boise, Jay Lundell, and Anna Foucek. 2008. Unobtrusive in-home monitoring of cognitive and physical health: Reactions and perceptions of older adults. *J. Appl. Geront.* 27, 2 (2008), 181–200. DOI: https://dx.doi.org/10.1177%2F0733464807311435

[10] Tiago D. P. Mendes, Radu Godina, Eduardo M. G. Rodrigues, Joao C. O. Matias, and Joao P. S. Catalao. 2015. Smart home communication technologies and applications: Wireless protocol assessment for home area network resources. *Energies.* 8, 7 (2015), 7279–7311. DOI: http://dx.doi.org/10.3390/en8077279

[11] Luis E. Anido, Sonia M. Valladares, Manuel J. Fernandez-Iglesias, Carlos Rivas, and Miguel Gomez. 2013. Adapted interfaces and interactive electronic devices for the smart home. In *Proceedings of the 8th International Conference on Computer Science & Education.* 472–477. DOI: https://doi.org/10.1109/ICCSE.2013.6553957

[12] Mohamed Asma Ben Hadj, Val Thierry, Andrieux Laurent, and Kachouri Abdennaceur. 2012. Using a Kinect WSN for home monitoring: Principle, network and application evaluation. In *Proceedings of the International Conference on Wireless Communications in Underground and Confined Areas (ICWCUCA).* 1–5. DOI: https://doi.org/10.1109/ICWCUCA.2012.6402487

[13] Nikhil Naikal, Pedram Lajevardi, and S. Sastry Shankar. 2014. Joint detection and recognition of human actions in wireless surveillance camera networks. In *Proceedings of the IEEE International Conference on Robotics and Automation (ICRA).* 4747–4754. DOI: https://doi.org/10.1109/ICRA.2014.6907554

[14] Hsien-Po Shiang and Mihaela van der Schaar. 2010. Information-constrained resource allocation in multicamera wireless surveillance networks. *IEEE Trans. Circ. Syst. Video Tech.* 20, 4 (2010), 505–517, DOI: https://doi.org/10.1109/TCSVT.2009.2035837

[15] Nikos Komninos, Eleni Philippou, and Andreas Pitsillides. 2014, A survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Commun. Surv. Tutor.* 16, 4 (2014), 1933–1954. DOI: https://doi.org/10.1109/COMST.2014.2320093

[16] Taewan Kim, Hyungsoo Park, and Yunmo Chung. 2013. Integrated system of face recognition and sound localization for a smart door phone. *IEEE Trans. Consum. Electron.* 59, 3 (2013), 598–603. DOI: https://doi.org/10.1109/TCE.2013.6626244

[17] Geng Yang, Jian Xu, Wei Chen, Zheng-Hua Qi, and Hai-Yong Wang. 2010. Security characteristic and technology in the internet of things. *Journal of Nanjing University of Posts and Telecommunications (Natural Science).* 30, 4 (2010), 20–29.

[18] Hui Suo, Jiafu Wan, Caifeng Zou, and Jianqi Liu. 2012. Security in the Internet of Things: A review. In *Proceedings of the International Conference on Computer Science and Electronics Engineering (ICCSEE).* 648–651. DOI: https://doi.org/10.1109/ICCSEE.2012.373

[19] Francois Carrez, Martin Bauer, Mathieu Boussard, Nicola Bui, Christine Jardak, Jourik De Loof, Carsten Magerkurth, Stefan Meissner, Andreas Nettsträter, Alexis Olivereau, Matthias Thoma, Joachim W. Walewski, Julinda Stefa, and Alexander Salinas. 2013. IoT-A deliverable D1.5-final architectural reference model for the IoT v3.0. Retrieved May 2017 from http://www.meet-iot.eu/deliverables-IOTA/D1_5.pdf.

[20] Tobias Zillner. 2015. Zigbee exploited. *The Good, the Bad and the Ugly.* Retrieved May 2017 from https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf.

[21] Daniel Schwarz. 2016. The current state of security in smart home systems, threats in the internet of things. *SEC Consult Vulnerability Lab – Vienna.* Retrieved May 2017 from https://www.sec-consult.com/.

[22] Subha Koley and Prasun Ghosal. 2015. Addressing hardware security challenges in internet of things: recent trends and possible solutions. In *Proceedings of the IEEE 12th International Conference on Ubiquitous Intelligence and Computing and 2015 IEEE 12th International Conference on Autonomic and Trusted Computing and 2015 IEEE 15th International Conference on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom)*. 517–520. DOI: https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP.2015.105

[23] Orlando Arias, Jacob Wurm, Khoa Hoang, and Yier Jin. 2015. Privacy and security in internet of things and wearable devices. *IEEE Trans. Multi-Scale Comput. Syst.* 1, 2 (2015), 99–109. DOI: https://doi.org/10.1109/TMSCS.2015.2498605

[24] Sachin Minocha. 2013. WBAN and its applications. *Internat. J. Engin., Manage., Human. Social Sci. Parad. (IJEMHS)*, 2, 1, ISSN: 2347–601X.

[25] Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, and David Wagner. 2016. Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM Asia Conference on Computer and Communications Security (ASIA CCS)*. ACM, New York, 461–472. DOI: https://doi.org/10.1145/2897845.2897886

[26] Georgios Mantas, Dimitrios Lymberopoulos, and Nikos Komninos. 2011. Security in smart home environment. In *Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications*, Athina Lazakidou, Konstantinos Siassiakos, and Konstantinos Ioannou (Eds.). 171–190. DOI: https://doi.org/10.4018/978-1-61520-805-0

[27] Xun Wang, Wenjun Gu, Kurt Schosek, Sriram Chellappan, and Dong Xuan. 2004. Sensor network configuration under physical attacks. *Int. J. Ad Hoc Ubiq. Comput.* 4, 3–4 (2004), 174–182. DOI: https://doi.org/10.1504/IJAHUC.2009.02452

[28] Sajal Das, Krishna Kant, and Nan Zhang. 2012. *Handbook on Securing Cyber-Physical Critical Infrastructure: Foundation and Challenges*. Morgan Kaufmann, Boston, MA. ISBN: 9780124159105

[29] Rodrigo Roman, Pablo Najera, and Javier Lopez. 2011. Securing the Internet of Things. *IEEE Comput.* 44, 9 (2011), 51–58. DOI: https://doi.org/10.1109/MC.2011.291

[30] Michele Zorzi, Alexander Gluhak, Sebastian Lange, and Alessandro Bassi. 2010. From today's INTRAnet of Things to a future Internet of Things: A wireless- and mobility-related view. *IEEE Wireless Commun.* 17, 6 (2010), 44–51. DOI: https://doi.org/10.1109/MWC.2010.5675777

[31] Kashif Gill, Se HoonYang, and Wei Wang. 2012. Scheme for preventing low-level denial-of-service attacks on wireless sensor network-based home automation systems. *IET Wireless Sensor Systems.* 2, 4 (2012), 361–368. DOI: https://doi.org/10.1049/iet-wss.2011.0177

[32] R. Kowsik and L. Vignesh. 2016. Mitigating insider data theft attacks in the cloud. In *Proceedings of the 2016 2nd International Conference on Science Technology Engineering and Management (ICONSTEM)*. 2016, 561–567. DOI: https://doi.org/10.1109/ICONSTEM.2016.7560956

[33] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. 2016. Security analysis of emerging smart home applications. In *Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP)*. 636–654. DOI: https://doi.org/10.1109/SP.2016.44

[34] Elaine B. Barker and Allen L. Roginsky. 2011. SP 800-131A Revision 1. Transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths, national institute of standards & technology. Retrieved May 2017 from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800−131Ar1.pdf.

[35] Eric Rescorla and Nagendra Modadugu. 2012. RFC 6347. Datagram transport layer security version 1.2. Retrieved May 2017 from https://tools.ietf.org/html/rfc6347.

[36] Urs Hunkeler, Hong Linh Truong, and Andy Stanford-Clark. 2008. MQTT-S A publish/subscribe protocol for wireless sensor networks. In *Communication Systems Software and Middleware and Workshops (COMSWARE 2008)*. 2008, 791–798. DOI: https://doi.org/10.1109/COMSWA.2008.4554519

[37] Z. Shelby, K. Hartke, and C. Bormann. 2014. RFC 7252. The constrained application protocol (CoAP). Retrieved May 2017 from https://tools.ietf.org/html/rfc7252.

[38] Sye Loong Keoh, Sandeep S. Kumar, and Hannes Tschofenig. 2014. Securing the Internet of Things: A standardization perspective. *IEEE Internet of Things J.* 1, 3 (2014), 265–275. DOI: https://doi.org/10.1109/JIOT.2014.2323395

[39] Diego Altolini, Vishwas Lakkundi, Nicola Bui, Cristiano Tapparello, and Michele Rossi. 2013. Low power link layer security for IoT: Implementation and performance analysis. In *Proceedings of Wireless Communications and Mobile Computing Conference (IWCMC)*. July 2013, 919–925. DOI: https://doi.org/10.1109/IWCMC.2013.6583680

[40] Quangang Wen, Xinzheng Dong, and Ronggao Zhang. 2012. Application of dynamic variable cipher security certificate in Internet of Things. In *Proceedings of Cloud Computing and Intelligent Systems (CCIS)*. 2012, 1062–1066. DOI: https://doi.org/10.1109/CCIS.2012.6664544

[41] Mohit Sethi, Jari Arkko, and Ari Keränen. 2012. End-to-end security for sleepy smart object networks. In *Proceedings of the IEEE 37th Conference on Local Computer Networks Workshops (LCN Workshops)*. 2012, 964–972. DOI: https://doi.org/10.1109/LCNW.2012.6424089

[42] Ki-Woong Park, Sang Seok Lim, and Kyu Ho Park. 2008. Computationally efficient PKI-Based single sign-on protocol, PKASSO for mobile devices. *IEEE Trans. Comput.* 57, 6, 821–834. DOI: https://doi.org/10.1109/TC.2008.36

[43] Michael O. Rabin. 1979. Digitalized signatures and public-key functions as intractable as factorization. Massachusets Institute of Technology, MA, (January 1979). Tech. Rep.

[44] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. 1998. NTRU: A ring-based public key cryptosystem. In *Proceedings of the 3rd International Symposium on Algorithmic Number Theory (ANTS'98).* Lecture Notes in Computer Sciences, vol. 1423, Springer, Berlin, Germany, 267–288.

[45] Victor S. Miller. 1985. Use of elliptic curves in cryptography. In *Proceedings of the CRYPTO'85 Advances in Cryptology.* Lecture Notes in Computer Sciences. Springer, Berlin, Germany, 1985, 417–426. ISBN:3-540-16463-4

[46] Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid. 2012. *NIST special publication 800-57 Recommendation for Key Management. Part 1: General.* National Institute of Standards & Technology. Retrieved May 2017 from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800−57pt1r4.pdf.

[47] David. J. Malan, Matt Welsh, and Michael D. Smith. 2008. Implementing public-key infrastructure for sensor networks. *ACM Trans. Sensor Netw.* 4, 4 (2008), 22:1–22:23. DOI: https://doi.org/10.1145/1387663.1387668

[48] Kai Han, Jun Luo, Yang Liu, and Athanasios V. Vasilakos. 2013. Algorithm design for data communications in duty-cycled wireless sensor networks: A survey. *IEEE Communications Magazine.* 51, 7, 107–113. DOI: https://doi.org/10.1109/MCOM.2013.6553686

[49] Mo Li, Zhenjiang Li, and Athanasios V. Vasilakos. 2013. A survey on topology control in wireless sensor networks: Taxonomy, comparative study, and open issues. *Proc. IEEE* 101, 12, 2538–2557. DOI: https://doi.org/10.1109/JPROC.2013.2257631

[50] Laurent Eschenauer and Virgil D. Gligor. 2002. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS'02).* ACM, New York, 41–47. DOI: http://dx.doi.org/10.1145/586110.586117

[51] Donggang Liu and Peng Ning. 2003. Establishing pairwise keys in distributed sensor networks. In *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS'03).* ACM, New York, 52–61. DOI: http://dx.doi.org/10.1145/948109.948119

[52] Sayantani Saha. 2015. Secure sensor data management model in a −sensor-cloud integration environment. In *Proceedings of the IEEE 2015 Applications and Innovations in Mobile Computing (AIMoC).* 158–163. DOI: https://doi.org/10.1109/AIMOC.2015.7083846

[53] Bartosz Przydatek, Dawn Song, and Adrian Perrig. 2003. SIA: Secure Information Aggregation in sensor networks. In *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys'03).* ACM, New York, 255–265. DOI: http://dx.doi.org/10.1145/958491.958521

[54] Sulabh Bhattarai, Linqiang Ge, and Wei Yu. 2012. A novel architecture against false data injection attacks in smart grid. In *Proceedings of the IEEE International Conference on Communications (ICC) (IEEE ICC'12).* 2012, 907–911. DOI: https://doi.org/10.1109/ICC.2012.6364511

[55] Yi Huang, Husheng Li, Kristy A. Campbell, and Zhu Han. 2011. Defending false data injection attack on smart grid network using adaptive CUSUM test. In *Proceedings of the IEEE 45th Annual Conference on Information Sciences and Systems.* 2011, 1–6. DOI: http://dx.doi.org/10.1109/CISS.2011.5766111

[56] Rathanakar Acharya and K. Asha. 2008. Data integrity and intrusion detection in wireless sensor networks. In *Proceedings of the IEEE ICON 16th IEEE International Conference on Networks.* 2008, 1–5. DOI: https://doi.org/10.1109/ICON.2008.4772642

[57] Caiming Liu, Jin Yang, Run Chen, Yan Zhang, and Jinquan Zeng. 2011. Research on immunity-based intrusion detection technology for the internet of things. In *Proceedings of the 7th International Conference on Natural Computation.* 2011, 212–216. DOI: https://doi.org/10.1109/ICNC.2011.6022060

[58] Caiming Liu, Y. Zhang, and H. Zhang. 2013. A novel approach to IoT security based on immunology. In *Proceedings of the 2013 9th International Conference on Computational Intelligence and Security (CIS).* 2013, 771–775. DOI: https://doi.org/10.1109/CIS.2013.168

[59] Mostafa M. Fouda, Zubair Md. Fadlullah, Nei Kato, Rongxing Lu, and Xuemin Sherman Shen. 2011. A lightweight message authentication scheme for smart grid communications. *IEEE Trans. Smart Grid* 2, 4, 675–685. DOI: https://doi.org/10.1109/TSG.2011.2160661

[60] Rucha Sule, Raj S. Katti, and Rajesh G. Kavasseri. 2012. Variable length fast message authentication code for secure communication in smart grids. In *Proceedings of the IEEE Power and Energy Society General Meeting.* 1-6. DOI: https://doi.org/10.1109/PESGM.2012.6345622

[61] Amar Rasheed and Rabi N. Mahapatra. 2012. The three-tier security scheme in wireless sensor networks with mobile sinks. *IEEE Trans. Paral. Distrib. Syst.* 23, 5, 958–965. DOI: https://doi.org/10.1109/TPDS.2010.185

[62] Komal Rege, Nikita Goenka, Pooja Bhutada, and Sunil Mane. 2013. Bluetooth communication using hybrid encryption algorithm based on AES and RSA. *Int. J. Comput. Applicat.* 2012, 71, 2. DOI: https://doi.org/ 10.5120/12617-9061

[63] Zhifeng Xiao, Yang Xiao, and David Hungchang Du. 2013. Non-repudiation in neighborhood area networks for smart grid. *IEEE Communications Magazine.* 51, 1, 18–26. DOI: https://doi.org/10.1109/MCOM.2013.6400434

[64] Tim Bray. The JavaScript Object Notation (JSON) Data Interchange Format, RFC 7159, March 2014.

[65] Michael Jones, J. Bradley, and N. Sakimura. 2015. RFC7515 JSON Web Signatures (JWS): Proposed Standards, 2015. Retrieved May 2017 from https://tools.ietf.org/html/rfc7515.

[66] Rudolf Volner, Petr Bores, and Vladimir Smrz. 2008. A product based security model for smart home appliances. In *Proceedings of the Biennial Baltic Electronics Conference.* 2008, 221–222. https://doi.org/10.1109/BEC.2008.4657519

[67] Lujo Bauer, Lorrie Faith Cranor, Robert W. Reeder, Michael K. Reiter, and Kami Vaniea. 2009. Real life challenges in access-control management. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'09)*. ACM, New York, 899–908. DOI: https://doi.org/10.1145/1518701.1518838

[68] A. J. Bernheim Brush, Jaeyeon Jung, Ratul Mahajan, and Frank Martinez. 2013. Digital neighborhood watch: Investigating the sharing of camera data amongst neighbors. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work (CSCW'13)*. ACM, New York, 693–700. DOI: https://doi.org/10.1145/2441776.2441853

[69] Haodong Wanga and Qun Li. 2006. Distributed user access control in sensor networks. In *Proceedings of the International Conference on Distributed Computing in Sensor Systems (DCOSS'06)*. Lecture Notes in Computer Science, 2006, 4026. DOI: https://doi.org/10.1007/11776178_19

[70] Himanshu Khurana, Rakesh Bobba, Tim Yardley, Pooja Agarwal, and Erich Heine. 2010. Design principles for power grid cyber infrastructure authentication protocols. In *Proceedings of the 43rd Hawaii International Conference on System Sciences* (Honolulu, HI, 2010), 1–10. DOI: https://doi.org/10.1109/HICSS.2010.136

[71] Sushmita Ruj, Amiya Nayak, and Ivan Stojmenovic. 2011. A Security Architecture for Data Aggregation and Access Control in Smart Grids, CoRR, 2011, 1–12, arXiv:1111.2619.

[72] Jun Wu, Mianxiong Dong, Kaoru Ota, Zhenyu Zhou, and Bin Duan. 2014. Towards fault-tolerant fine-grained data access control for smart grid. *Wirel. Pers. Commun.* 75, 3 (April 2014), 1787–1808. DOI: http://dx.doi.org/10.1007/s11277-013-1294-6

[73] Rune Hylsberg Jacobsen, Søren Aagaard Mikkelsen, and Niels Holm Rasmussen. 2015. Towards the use of pairing-based cryptography for resource-constrained home area networks. In *Proceedings of the 2015 Euromicro Conference on Digital System Design (DSD).* IEEE, 2015, 233–240. DOI: https://doi.org/10.1109/DSD.2015.73

[74] Theis Solberg Hjortha and Rune Torbensen. 2012. Trusted domain: A security platform for home automation. *Computers & Security* 2012, 31, 8, 940–955. DOI: http://dx.doi.org/10.1016/j.cose.2012.07.003

[75] Johannes Gilger and Hannes Tschofenig. 2014. RFC 7397. Report from the smart object security workshop. Retrieved May 2017 from https://tools.ietf.org/html/rfc7397.

[76] Fibaro Motion Sensor FGMS-001 Operating Manual. Retrieved May 2017 from: http://manuals.fibaro.com/content/manuals/en/FGMS-001/FGMS-001-EN-T-v2.0.pdf.

[77] Y. Nir and A. Langley. 2015. RFC 7539. ChaCha20 and Poly1305 for IETF Protocols, May 2015. Retrieved May 2017 from: https://tools.ietf.org/html/rfc7539.

Received June 2016; revised May 2017; accepted July 2017